INFORMATION SECURITY OFFICER: SPELEN MET INVLOED

Informatiebeveiliging is een kwaliteitsaspect dat verbonden is aan bijna alles wat zich in een organisatie afspeelt. Als Information Security Officer vervul je een centrale rol en word je geconfronteerd met de meest uiteenlopende vraagstukken en risico's. Je invloed is echter niet vanzelfsprekend, en je ontleent deze vaak niet aan je hiërarchische positie. Je zult je gezags- of autoriteitspositie moeten verdienen én behouden. Maar let op, verdienen is iets anders dan afdwingen. Het vergroten van je invloed zonder in de afdwing-valkuil te stappen kan een behoorlijke uitdaging zijn.

Je kunt iedereen het spreekwoordelijke mes op de keel zetten om dingen voor elkaar te krijgen, maar na een paar maanden wil niemand meer met je samenwerken en lunch je alleen. Vanuit de inhoud gezien heb je waarschijnlijk gelijk en horen die risico's zo snel mogelijk te worden behandeld. Wil je echter op de lange termijn succesvol blijven, dan zul je anders te werk moeten gaan. Dit begint met het besef dat een goede relatie met je collega's cruciaal is voor een goede informatiebeveiliging. Wanneer je als bikkelharde handhaver door de organisatie trekt, dan zullen deze collega's je doorgaans (bewust of onbewust) buitenspel proberen te zetten. Uitzonderingen daargelaten is dat niet de wijze waarop je je invloed wilt vergroten. Het geeft wellicht resultaten op de korte termijn, maar je verspeelt op deze manier wel je eigen houdbaarheid.

Goede beveiliging niet vanzelfsprekend

Veel organisaties kenmerken zich tegenwoordig door de aanwezigheid van tegenstelde belangen, een sterke focus op functionele vernieuwing, werken onder hoge tijdsdruk, en een klantvraag die centraal staat. Hartstikke prima, maar niet wanneer beheer- en onderhoudswerkzaamheden van het bestaande ICT-landschap hieronder lijden. Deze vormen namelijk de basis voor een betrouwbare informatievoorziening, en wanneer de noodzakelijke aandacht hiervoor ontbreekt hopen de risico's zich in hoog tempo op.

Als Information Security Officer voel je dat het tijd is om in actie te komen, maar de ervaring leert dat dit niet gemakkelijk is. Een gedragen informatiebeveiligingsproces ontbreekt, de budgetten en beschikbare handjes voor het komende jaar zijn al grotendeels vergeven, en er is structureel geen prioriteit voor het implementeren van risico-mitigerende maatregelen. Inhoudelijk heb je een sterk verhaal met goede argumenten, maar op de werkvloer word je vaak ervaren als degene die kritische vragen stelt op een moment dat niemand erop zit te wachten. En omdat er doorgaans geen sprake is van een hiërarchische verhouding met je collega´s, zul je je omgeving op een andere wijze moeten beïnvloeden.

Begrijp het spel

Inhoudelijke kennis is absoluut noodzakelijk, maar niet de enige succesfactor. Op de juiste manier participeren in ´het spel´ wat zich dagelijks binnen de organisatie afspeelt, is minstens zo belangrijk. Investeer daarom ook in het begrijpen van de formele én informele context waarbinnen je opereert. Hoe loopt de besluitvorming? Wie zijn de spelers in het politiek bestuurlijke krachtenveld? Voor welke argumenten zijn ze gevoelig? Hoe reageren ze op elkaar? Wie trekt er achter de schermen aan de touwtjes? Hoe krijg je iemand het beste in beweging? Welk wisselgeld kun je hiervoor inzetten?

De antwoorden op dergelijke vragen geven inzicht in het politieke en culturele karakter van de organisatie, en helpen je om de paden naar jouw succes (acceptabele risico's) te kunnen bepalen. Maar het moeilijkste moet dan nog komen, en dat is het spelen van het spel. Pas wanneer dit lukt, ben je in staat jouw inhoudelijke kennis optimaal te benutten.

Verleiden zonder cadeautjes

Participeren in het spel is bepaald geen sinecure. Dit is met regelmaat de plek waar de tegengestelde belangen boven komen drijven en er wordt gevochten voor elke centimeter. Voor je het weet ben je getuige van het betere ellebogenwerk en doordachte politieke manoeuvres.

Omdat de reikwijdte van je invloed binnen het spel zich zelden beperkt tot de collega's met een formele rol in het besluitvormingsproces, is het belangrijk om met iedereen een goede relatie te onderhouden en continu te werken aan het vergroten van je autoriteitspositie. Deze zaken zijn namelijk bepalend voor de mate waarin collega's bereid zijn hun medewerking te verlenen, of zich openlijk achter je standpunt willen/durven scharen.

Kortom, als je eruit wil halen wat erin zit, heb je je collega's hard nodig. Maar hoe vergroot je nou je autoriteitspositie zonder de relatie met je collega's onder druk te zetten? De vele variabelen die van invloed zijn, maken het beantwoorden van deze vraag

Dennis Baaten is Security Consultant bij Baaten ICT Security. Dennis is bereikbaar via dennis@baaten.com

complex. Toch kun je als Information Security Officer een aantal dingen doen die bijdragen aan het vergroten van je autoriteitspositie, zonder dat daarmee je eigen houdbaarheid in het geding komt.

- **Beleid op orde** – zorg dat het informatiebeveiligingsbeleid op orde is, en zo hoog mogelijk in de hiërarchische boom is goedgekeurd. Dit voorkomt onnodige discussies, en helpt je bij het pareren van vragen zoals "waar staat dan dat dit moet?."

- **Aansluiten bij kernwaarden van de organisatie** – probeer tijdens het formuleren en/of onderbouwen van informatiebeveiligingsdoelen aansluiting te zoeken bij de kernwaarden van je organisatie. In de regel ontstaat hierover namelijk minder discussie omdat (bijna) iedereen deze erkent en niet zo snel zal tegenspreken.

- **Zichtbaarheid** – maak jezelf zo zichtbaar mogelijk. Bijvoorbeeld door aan te haken bij teamoverleggen, bilaterale overleggen met het management, of door het organiseren van awareness- en demosessies. Ga eens een dagje 'zwerven' op de werkvloer en toon interesse in het werk wat collega's doen. Leg contact, stel open vragen, en luister.

- **Geef complimenten** – je wordt verwacht kritisch te zijn, maar spreek het ook uit wanneer iets goed gaat. Een schouderklopje voor de beheerder die de nieuwe Java-patches snel heeft uitgerold, of een compliment voor de applicatiebeheerder die zijn autorisatiematrix goed op orde heeft. Voorkom dat de dingen uit jouw mond uitsluitend negatief zijn.

- **Practice what you preach** – het zijn vaak kleine simpele dingen, maar houd je aan je eigen regels. Vergrendel je pc bij het verlaten van je werkplek, zorg voor een schoon en opgeruimd bureau als er geen slot op de deur zit, gebruik geen cloud-diensten als je dat ook van je collega's verwacht. Je wilt niet uitstralen dat je het zelf allemaal niet zo nauw neemt met het volgen van de regels. Als jij je niet aan de regels houdt, komt er een moment dat dit tegen je wordt gebruikt.

- **Betrokken maar niet verantwoordelijk** – beleg de verantwoordelijkheid waar deze thuis hoort; zo dicht mogelijk bij de operatie. Blijf nauw betrokken, maar zorg dat de verantwoordelijkheid voor bijvoorbeeld het implementeren van maatregelen niet bij jou terecht komt. De Information Security Officer is nooit de probleem- of risico-eigenaar. Benadruk de verantwoordelijkheid van je collega's, maar biedt altijd aan om ze te helpen deze verantwoordelijk te nemen. Geef die credits maar één keer weg; help iemand een goede beurt te maken bij zijn/haar leidinggevende. Denk vanuit het belang van de organisatie.

- **Betrek de risico-eigenaar** – houd je niet alleen bezig met de ICT-afdeling (de aanbodzijde), maar betrek ook actief de business (de vraagzijde). Maak de business risicobewust, zodat deze de rol van risico-eigenaar op zich kan nemen. Een klant die vraagt om een goede beveiliging helpt enorm om de ICT-afdeling in beweging te krijgen. Zeker in omgevingen waar de klantvraag expliciet centraal wordt gesteld.

- **De eigenaar bepaalt risicobereidheid** – borg dat besluiten omtrent risico's op de juiste plek in de organisatie worden genomen; bij de risico-eigenaar. Deze bevindt zich zelden in de ICT-afdeling, maar bijna altijd bij de business. Wanneer de ICT-afdeling autonoom risico's wenst te behandelen, zonder de risico-eigenaar te betrekken, kunnen risico's uitsluitend worden verlaagd door het implementeren van (aanvullende) maatregelen. Alleen de eigenaar kan risico's accepteren. Vraag hierbij altijd om een risicoanalyse op basis waarvan het akkoord is gegeven. Enerzijds is dit de vastlegging van een geaccepteerd risico, en anderzijds geeft dit aan of de eigenaar goed heeft begrepen wat het risico inhoudt.

- **Risico-eigenaar betaalt de rekening** – een eigen budget kan voordelen hebben, maar is vaak ook een risico. Wanneer er met budgetten wordt gewerkt, zorg dan dat jij niet de budgethouder voor informatiebeveiliging bent. Hiermee voorkom je dat de implementatie van risico-mitigerende maatregelen afhankelijk wordt van jouw potje met geld. Een dergelijke directe betrokkenheid bij de uitvoering van het informatiebeveiligingsbeleid is niet gewenst.

- **Blijf die (tegen)druk geven** – jij stelt kritische vragen op momenten dat het anderen niet uitkomt. Dat hoort erbij, is gezond voor een organisatie, en zal nooit verdwijnen. Je behartigt nu eenmaal een belang binnen de organisatie wat vaak wordt ervaren als strijdig met andere belangen. Bij aanhoudende druk en uitblijvende resultaten, komt er een moment dat je collega's (vaak het management) zullen proberen om jouw druk te verminderen. Bekijk of het verstandig is je collega's tegemoet te komen, maar laat de druk niet (helemaal) wegvallen. Zonder druk stagneert vaak ook de voortgang, en dan kun je opnieuw beginnen.

- **Geef en neem op het juiste moment** – weet wanneer je op je strepen moet gaan staan, en zoek naar de juiste balans tussen geven en nemen. Ga je te vaak op je strepen staan (de bikkelharde handhaver) zonder dat dit het juiste effect sorteert, dan verliest dit voor je omgeving zijn waarde. Geef je teveel ruimte, dan word je ook niet serieus genomen. Bepaal

voor jezelf welk wisselgeld je hebt, en houd voet bij stuk wanneer het urgente risico's betreft die ook zo worden ervaren.

- **Onafhankelijke hiërarchische positie** – probeer met je hiërarchische positie je onafhankelijkheid te vergroten. Bij voorkeur dus niet binnen de ICT-afdeling, en wanneer dat wel zo is, dan liever in de staf in plaats van de lijn. In de basis geldt: creëer zoveel mogelijk afstand tussen jezelf en het organisatieonderdeel waarover je je het vaakst kritisch uitspreekt (en dat verantwoordelijk is voor de uitvoering). Dit voorkomt (de schijn van) belangenverstrengelingen.

Blijf jezelf

Bovenstaande tips kunnen je helpen je effectiviteit als Information Security Officer te doen toenemen. Je wordt langzaam een informele autoriteit, met als gevolg dat je het spel gemakkelijker mee kunt spelen. Maar neem niets voor lief, en vergeet niet dat je voor het realiseren van een acceptabel risiconiveau grotendeels bent aangewezen op je eigen vaardigheden en inzichten. Bedenk hierbij dat organisaties zelden statisch zijn. Het vinden van de juiste modus waarin jouw toegevoegde waarde optimaal is, is een continu proces dat gepaard gaat met vallen en opstaan. Behaalde resultaten in het verleden bieden ook hier geen garantie voor de toekomst; morgen kan het zomaar anders zijn.

Het allerbelangrijkste is dat je jezelf blijft. Iedereen heeft een uniek karakter met voor- en nadelen die van invloed zijn op je gedrag. Uiteraard kun je leren je gedrag in jouw voordeel aan te passen, maar pas op dat je hiermee niet te ver van jezelf af komt te staan. Een goede manager/coach begrijpt dit en helpt je, binnen de kaders van je persoonlijkheid, met het optimaal leren benutten van je krachten. Wees creatief en voorkom dat je continu gedrag moet vertonen wat niet bij je past. Dat houd je niet vol en is bovendien geen prettig vooruitzicht wanneer de wekker 's ochtends weer afgaat.